REMARKS

Please reconsider the present application in view of the above amendments and following remarks. Applicant thanks the Examiner for carefully considering the present application.

I. Disposition of the Claims

Claims 1-17 and 20-33 are currently pending in the present application. By way of this reply, claims 1, 12, 27, and 30-33 have been amended.

II. Objection(s) to the Specification

The Specification was objected to as failing to provide proper antecedent basis for certain subject matter in claims 12 and 32. However, as shown in the amendments above, claims 12 and 32 have been amended to remedy the objections raised by the Examiner. Accordingly, withdrawal of the objections to the Specification is respectfully requested.

III. Rejection(s) under 35 U.S.C. § 112

Claims 12-17 and 32 were rejected under 35 U.S.C. § 112, first paragraph, as failing to comply with the written description requirement. However, these rejections are now moot in view of the amendments to claims 12 and 32 shown above. Accordingly, withdrawal of the § 112 rejections is respectfully requested.

IV. Rejection(s) under 35 U.S.C. § 102

Claims 1-10 and 12-33 were rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,721,721 ("Bates"). For the reasons set forth below, these rejections are

respectfully traversed.

Independent claim 1 in part requires "determining the executability of [] computer content in response to the result of comparing a time stamp of [the] computer content with [a] first computer virus alert time". Further, as recited in claim 1, the virus alert time is determined effectively in response to a "virus outbreak report indicating a virus attack threat to a computer network". Independent claims 12 and 31-33 recite similar language.

Further, independent claim 20 in part requires "specifying an access control rule for blocking the execution of suspicious or susceptible computer contents that are time-stamped not before [a] computed virus alert time". Further, as recited in claim 20, the virus alert time is computed effectively in response "virus outbreak report indicating a virus attack threat to a computer network". Independent claims 27 and 30 recite similar language.

Bates purportedly discloses a system that integrates virus checking functionality into a computer database search environment, thereby decreasing the risks of viruses associated with accessing search results from computer database searches. *See* Bates, Abstract; column 3, lines 1-3. With reference to Figure 2 of Bates, a user provides a virus criterion by which search results can be displayed. As to this virus criterion, Bates states:

> The virus criterion obtained from the user typically specifies the rule by which files represented in a result set are to be indicated as being "untrustworthy", i.e., of presenting a comparatively higher risk of viral infection. The virus criterion, for example, may be based simply upon whether or not a file represented in a result set has been found to contain a virus. The virus criterion may also specify whether a file has been virus checked within a predetermined period of time, such that files that have not been found to be infected with a virus, yet have not been checked for a lengthy period of time, are still not considered trustworthy. The virus criterion may also specify whether a file has been changed since the last time a virus check was performed, such that modified files will not be considered to be trustworthy until they are re-checked. In addition, a period of time during which a file has been found to be free of viral infection may also be specified, such that files that were previously found to present a greater risk of a virus may still obtain trustworthy status after expiration of a sufficient period of time during

which no viruses are found.

See Bates, column 9, line 56 – column 10, line 8. Thus, as related to "time" in Bates, the user can assess the "trustworthiness" of a search result file by setting a virus criterion as to (i) whether the file has been virus checked within a predetermined period of time, (ii) whether the file has been changed since the last time a virus check was performed, or (iii) whether a particular period of time has elapsed in which the file has been found to be free of viral infection. Element 210 in Figure 7 of Bates shows how a user may select such virus criterion. *See* Bates, column 17, lines 35-50.

While Bates discloses the above virus criteria, Bates is completely silent as to comparing or assessing a time stamp of a returned search result file against *a computed virus alert time*. As described in the present application, a virus alert time is computed when, for example, there is a virus outbreak report indicating a virus attack threat to a network. *See* Specification, paragraphs [0034], [0038], [0067]. For computer content attempting or expected to execute, a time stamp of that computer content is compared against the computed virus alert time in order to prevent execution of the computer content if its time stamp is not before the virus alert time. *See* Specification, paragraph [0038]. In Bates, there is no disclosure of computing and/or comparing against a virus alert time; instead, Bates discloses: "comparing a current timestamp with a revision date" for "determining whether a file has been updated from a prior point in time" (*see* Bates, column 12, lines 59-62); storing "a timestamp (indicating when the URL was last checked for viruses)" (*see* Bates, column 13, lines 29-30; column 14, lines 47-48); searching for a "URL that is about to expire – that is, a URL having a timestamp that exceeds a predetermined threshold, indicating that the URL needs to be re-checked" (*see* Bates, column 16, lines 43-47); and "a timestamp indicating when the trustworthiness of the URL was determined via virus

checking" (*see* Bates, column 17, lines 20-22). As to the "relative time parameters" termed by the Examiner with reference to Figure 2 of Bates, these simply provide a manner by which a user can specify a virus criterion for determining file "trustworthiness" (e.g., "virus found in last 7 days", "not checked in last 14 days"). Bates is concerned with determining trustworthiness of a file based on whether that particular file was virus checked or not within or since some period of time. Bates is silent as to computing and comparing against a "virus alert time" computed/determined in response to a virus outbreak report indicating a virus attack threat to a computer network. Thus, Bates necessarily cannot disclose "determining the executability of computer content in response to the result of *comparing a time stamp of the computer content with [a] computer virus alert time*" as required by independent claims 1, 12, and 31-33. For at least the same reasons, Bates fails to at least disclose "specifying an access control rule for *blocking the execution of . . . computer contents that are time-stamped not before [a] computed virus alert time*" as required by independent claims 20, 27, and 30.

In view of the above, Bates fails to disclose each and every limitation recited in independent claims 1, 12, 20, 27, and 30-33. Thus, independent claims 1, 12, 20, 27, and 30-33 are patentable over Bates. Dependent claims are allowable for at least the same reasons. Accordingly, withdrawal of the § 102 rejections is respectfully requested.

V. Rejection(s) under 35 U.S.C. § 103

Claim 11 was rejected under 35 U.S.C. § 103(a) as being unpatentable over Bates in view of the document entitled "Norton Antivirus Corporate Edition" (1999, Version 1, pages 15, 22) ("Norton Antivirus (1999)"). For the reasons set forth below, this rejection is respectfully traversed.

Like Bates, Norton Antivirus (1999), fails to disclose all the limitations of independent claim 1 or supply that which Bates lacks. Namely, Norton Antivirus (1999) fails to disclose the "comparing a time stamp of the computer content with [a] computer virus alert time" limitation of independent claim 1 discussed above. Thus, Bates and Norton Antivirus (1999), whether taken singly or in combination, fail to disclose each and every limitation of independent claim 1. Independent claim 1 is therefore patentable over Bates and Norton Antivirus (1999). Dependent claim 11 is allowable for at least the same reasons. Accordingly, withdrawal of the § 103 rejection of claim 11 is respectfully requested.

V. Conclusion

The Examiner is encouraged to contact the undersigned attorney if it would beneficial to further advance the prosecution of the application.

Please apply any charges not covered, or any credits, to Deposit Account 19-2555 (Reference No. 20423-05957).

Respectfully Submitted,
Carey S. Nachenberg et al.

Date: September 1, 2006

By: /Wasif H. Qureshi/

Wasif H. Qureshi, Attorney of Record
Registration No. 51,048
FENWICK & WEST LLP
801 California Street
Mountain View, CA 94041
Phone: (650) 335-7121
Fax: (650) 938-5200